Site Authorization Service (SAZ) at Fermilab

Vijay Sekhri and Igor Mandrichenko
Fermilab

CHEP03, March 25, 2003

What is SAZ ?

- Site AuthoriZation service
- Think of it as something like an NIS level abstraction above the individual password file on each system.

Why is it needed ?

- In the GTK2, authorization is dealt with via the gridmapfile and there is one per service.
- Sites wish to impose sitewide policy centrally
- Can streamline some maintenance (eg. CRL checking)
- Allows for multiple layers of authorization

What does SAZ look like ?

SAZ

User Reg.

SAZ service

Admin

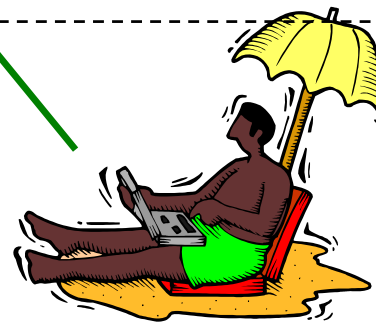
Db Interface

Db

Gridmapfile

Gatekeeper

Job Manager Job



What does it do ?

- The primary purpose for SAZ is to act as an authorization service for all Grid Resources on a site so that common policy can be enforced.
- A secondary purpose is to centralize maintenance of Certificate Revocation Lists (CRLs)
- The current version implements this in the gatekeeper via an LCAS (from the EDG suite of products) shared memory module.

What more does it do ?

- The service needs to get data about which DNs map to the same person.
- The internal SAZ database is populated through two interfaces: user and admin.
  - Users can add or delete their own DN.
    - We use Kerberos authentication for that transaction.
    - They may add several different DNs to their entry
  - Administrators can add or delete any entry in the database.

What is the status ?

- Prototype has been tested with EDG gatekeeper.
- Now being installed on CMS development testbed and soon on CDF/DO grids
- Specification for site authorization callout has been agreed between Globus, EDG, Virginia Tech, and FNAL teams and will come with next update of Globus 2

What is planned ?

- Move to standard callout (testing code now)
- Collaborate with EDG efforts to make common package of LCAS/VOMS/VO registration (this summer)
- Move to web services (GTK 3) in the Fall